MMS:ELM
F.#2017R00459

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

17 M 331

IN THE MATTER OF THE SEARCH OF APPLE IPHONE 5, MODEL NUMBER MD298B/A, IMEI NUMBER 01340300 9857104	APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, DANIEL SYMONDS, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been for approximately eight years. I am currently assigned to the NYC Airport BEST Financial Group. Previously, I served on the El Dorado Task Force, which targets financial crime at all levels and coordinates major money laundering investigations in the United States. During my tenure with HSI, I have investigated various violations, including but not limited to cash smuggling and money laundering, and I am presently responsible for conducting and assisting HSI investigations into the activities of individuals and

criminal groups responsible for financial crimes, including bulk cash smuggling. As a federal agent, I am authorized to execute – and have participated in the execution of – search warrants and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

3. I have received training in the area of bulk cash smuggling and have, as part of my daily duties as an HSI Special Agent, investigated violations related to bulk cash smuggling, including violations pertaining to the smuggling of cash from a place inside the United States to a place outside the United States, in violation of Title 31, United States Code, Sections 5316(a)(1)(A), 5316(b), and 5332.

4. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from my personal participation in this investigation and reports made to me by other law enforcement authorities. When I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. The property to be searched is an APPLE IPHONE 5, MODEL NUMBER MD298B/A, IMEI NUMBER 01340300 9857104, hereinafter the "Device." The Device is currently in the custody of HSI within the Eastern District of New York.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

8. On or about February 28, 2017, Customs and Border Protection ("CBP") officers assigned to the John F. Kennedy International Airport in Queens, New York ("JFK") were conducting outbound enforcement examinations for currency on Delta Airlines flight 42 ("Flight 42"), destined for Brussels, Belgium.

9. One of the passengers scheduled to depart on Flight 42, Salonica Rostas, checked three bags – one large red Lanson suitcase, one large blue Prestige suitcase and one medium blue Ormi suitcase. CBP officers conducted a currency examination of Rostas's luggage at the outbound luggage carousel. The examination of Rostas's red Landon suitcase revealed one red stuffed teddy bear and one white stuffed teddy bear. The examining CBP officers felt something unusual inside of each teddy bear. CBP officers cut open the teddy bears, and discovered a total of $50,000 in United States currency in the red bear and $40,000 in the white bear. Based on my training and experience, the concealment of currency within stuffed animals or other items that are not typically used to carry, contain or store other, additional objects is consistent with an intent to avoid detection of that currency by law enforcement.

10. During the course of the currency examination of Rostas's checked luggage, CBP officers also discovered $10,000 concealed in the pocket of a pair of gray/blue child-sized pants, and $4,950 in the pocket of a pair of tan child-sized pants. CBP officers discovered a total of $104,950 in United States currency in Rostas's checked luggage.

11. Subsequently, Rostas was encountered by CBP officers in the jet-way at JFK Terminal 4, Gate 38, while she was preparing to board Flight 42. The CBP officers were conducting outbound currency examinations with the assistance of a K-9 unit, K-9 Shey, trained to detect currency. K-9 Shey alerted positive for currency as to Rostas's carry-on bag, and Rostas was stopped for an examination.

12. Rostas was informed of the currency reporting regulations in English, and was advised that she was required to report all monies in her possession, including in her carry-on and checked luggage. She was advised to include any money she was carrying on behalf of another person. Rostas indicated that she understood the currency reporting requirements. She was presented with a Currency Reporting Flyer, CBP Form 909, in French (a language Rostas speaks fluently). Rostas orally reported that she was in possession of $1,000 in United States currency, wrote $1,000 on CBP Form 909, and signed it.

13. CBP officers asked Rostas to present all monies in her possession for verification, and she presented $1,040 in United States currency. She denied having any additional monies in her possession. A verification examination of her carry-on bag revealed an additional $22,844. In total, CBP seized $128,834 in United States currency from Rostas's checked and carry-on luggage.

14. HSI was notified and responded. HSI provided Rostas with her Miranda rights in English and in French, with the assistance of an interpreter. Rostas acknowledged that she understood her rights, and consented to a voluntary interview without the presence of counsel. A French interpreter was present throughout the interview. Rostas stated the following, in sum and substance and in part:

15. During the interview, Rostas stated that she arrived in New York on January 31, 2017. Rostas indicated that she had traveled to New York from Belguim with one checked bag, a green suitcase.

16. Rostas stated that she traveled to New York as a tourist, in order to see New York City and to go skiing. Upon arriving in New York, she stayed by herself in a hotel for approximately five days. She was not able to identify the hotel by name or address, and could not provide the street where the hotel was located. After about five days, Rostas was joined by her brother-in-law (who is the brother of her husband ("Brother-in-Law"), and his wife ("Sister-in-Law," and collectively the "In-Laws"). For the rest of Rostas's time in New York – approximately three weeks – she traveled around New York City with the In-Laws and stayed in various hotels. On February 14, 2017, Rostas and her In-Laws traveled to a ski resort somewhere in New York State for the day, and returned to New York City to spend the night in a hotel. All three individuals stayed in one room, and her Brother-in-Law paid for the hotel rooms with cash. Rostas was unable to identify the name of the ski resort, and could not provide any details about the hotels she stayed in while in New York City.

17. Rostas stated that she and her Sister-in-Law packed Rostas's bags for Flight 42 together, but her Sister-in-Law alone packed the money found in Rostas's checked baggage. However, Rostas was aware that the money was in her luggage (and concealed within stuffed animals) and knew the amount of money in her luggage before she checked her bags for Flight 42.

18. Rostas provided inconsistent explanations for why $90,000 was sewn inside of two stuffed animals in her checked suitcase. Initially she stated that money was secreted inside

of the teddy bears because she had previously lost luggage on flights to the Brussels airport. When asked why she would carry large sums of cash inside a bag she thought might be lost, Rostas stated that she thought her bags might arrive safely in Brussels because she was taking a direct (as opposed to a connecting) flight.

19. Rostas stated that all of the money in her checked and carry-on luggage, with the exception of $1,040, belonged to her Brother-in-Law. She stated that the remaining $127,794 represented the proceeds from the sale of her Brother-in-Law's home in Canada. Rostas stated that she was carrying this money to Belgium in anticipation of an upcoming trip she planned to take to Romania. Her Brother-in-Law wished to purchase a home in Romania, but would not arrive in Romania until some time after Rostas arrived. He asked Rostas to bring the cash with her to Romania, so that she could purchase the property he wished to buy there on his behalf.

20. At one point during the interview with HSI, Rostas offered to provide HSI with her Brother-in-Law's telephone number, so they could ask him about the money she was carrying in her checked and carry-on luggage. She produced a cellphone, an uncovered, white Apple iPhone, and indicated that she had stored a phone number for her Brother-in-Law therein. The number she had stored was associated with the sim card her Brother-in-Law used in his cellphone while he was in the United States. Rostas accessed her Brother-in-Law's cellphone number and provided it to HSI.

21. Rostas was released at the conclusion of the interview with HSI. CBP returned $1,000 of the $128,834 seized to Rostas for use as spending money.

22. On or about March 4, 2017, Rostas was arrested in Queens, New York, by HSI agents. The Device, an uncovered white Apple iPhone 5, was in Rostas's possession at the time, and was seized pursuant to her arrest. Based on my observations, training and experience, the Device is the same phone that was displayed by Rostas during her interview with HSI on or about February 28, 2017. Rostas was arraigned on a complaint on or about March 6, 2017, and released pursuant to a bond package. On or about March 30, 2017, a grand jury returned an indictment charging her with bulk cash smuggling, in violation of Title 31, United States Code, Sections 5332(a) and 5332(b).

23. Based on my education, training and experience, individuals involved in bulk cash smuggling typically communicate with one another about the cash smuggling scheme using their mobile electronic devices, including through telephone calls, text messages, electronic mails, and instant messaging applications. Indeed, during her February 28, 2017 interview with HSI, Rostas informed agents that a cellphone number for her Brother-in-Law (who, according to Rostas, gave her the money she attempted to smuggle out of the United States) was stored on the Device.

24. The Device is currently in the lawful possession of HSI. It came into HSI's possession incident to Rostas's arrest. Therefore, while HSI might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

25. The Device is currently in the possession of HSI within the Eastern District of New York. In my training and experience, I know that the Device has been stored in a manner in

which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of HSI.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

27. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

31. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

32. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Daniel Symonds

DANIEL SYMONDS
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
on April 13, 2017:

s/ Pollak

THE HONORA
UNITED STAT
EASTERN DIS

ATTACHMENT A

The property to be searched is an APPLE IPHONE 5, MODEL NUMBER MD298B/A, IMEI NUMBER 01340300 9857104, hereinafter the "Device." The Device is currently in the custody of HSI within the Eastern District of New York.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 31, United States Code, Sections 5316(a)(1)(A), 5316(b) and 5332 and involve Salonica Rostas since September 1, 2016, including:

a. All records and information on the Device described in Attachment A, including names and telephone numbers, as well as the contents of all call logs, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook or other social media posts or messages, Internet activity (including browser history, web page logs and search terms entered by the user), and other electronic media constituting evidence, fruits or instrumentalities of bulk cash smuggling in violation of;

b. All contact lists;

c. Passwords, encryption keys and other access devices that may be necessary to access the Device; and

d. Contextual information necessary to understand the evidence described in this attachment;

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.